Amendments to the Claims

This listing of claims will replace all prior versions and listing of claims in the application:

Listing of Claims

Claims 1 to 24 (cancelled)

Claim 25 (New): In a multicast capable Internet Protocol (IP) network comprising a plurality of interconnected routers, wherein specified ones of said plurality of interconnected routers each communicate with a decoy forwarding server (DFS) and a protected site router (PSR), and wherein said PSR is connected via a local area network (LAN) to a multicast receiver server (MRS) and a protected site server host (PSSH), a method of protecting against a coordinated distributed denial of service attack comprising:

(a) in standby mode, delivering unicast user traffic to said PSSH via said PSR; and

(b) upon detection of said distributed denial of service attack, at a selected one of said specified routers:

(i) decoying all traffic received at said specified router to said DFS, said traffic including said unicast user traffic and unicast attack traffic;
(ii) filtering said unicast user and attack traffic comprising identifying and discarding said unicast attack traffic;
(iii) encapsulating said unicast user traffic using a multicast address hopping protocol and delivering said encapsulated traffic to said MRS; and
(iv) de-encapsulating said encapsulated traffic and delivering said de-encapsulated traffic to said PSSH.

Claim 26 (New): The method of claim 25 wherein said multicast address hopping protocol comprises: (a) varying a chosen multicast IP address selected from a plurality of

multicast IP addresses according to a predetermined scheme known only to the DSF and MRS; and (b) communicating multicast packets on the chosen multicast IP address, wherein varying the chosen multicast IP address is initiated by a cryptographic key.

Claim 27 (New): The method of claim 25 further comprising, upon detection of a denial of service attack: (a) said MRS directing said PSR to cease advertising a route to said PSSH; and (b) said MRS directing said DFS to commence advertising a route to said PSSH.

Claim 28 (New): The method of claim 25 wherein said IP network comprises at least two autonomous systems communicating by way of a border router.

Claim 29 (New): The method of claim 25 further comprising, in addition to said filtering, moderating the arrival rate of said unicast user traffic to said PSSH.

Claim 30 (New): The method of claim 25 further comprising identifying the source of said unicast attack traffic utilizing a triangulation process, wherein said triangulation process comprises: (a) varying characteristics associated with said IP network to alter the flow of said unicast attack traffic; and (b) analyzing the resulting changes to determine the origin of said unicast attack traffic.

Claim 31 (New): The method of claim 1 wherein said distributed denial of service attack occurs at an upstream router and said filtering occurs at one or more downstream decoy forwarding servers.

Claim 32 (New): In a multicast capable Internet Protocol (IP) network, a system for protecting against a coordinated distributed denial of service attack comprising:

(a) a plurality of interconnected routers;

(b) a decoy forwarding server (DFS) and a protected site router (PSR) communicating with specified ones of said plurality of interconnected routers, wherein said DFS comprises a filter for identifying and discarding unicast attack traffic and a packet encapsulator for encapsulating unicast user traffic using a multicast address hopping protocol;

(c) a multicast receiver server (MRS) and a protected site server host (PSSH) communicating with said PSR via a local area network (LAN), wherein said MRS comprises a de-encapsulator for de-encapsulating said unicast user traffic received from said DFS and delivering said de-encapsulated traffic to said PSSH,

wherein, in standby mode, said specified one of said plurality of routers delivers unicast user traffic to said PSSH via said PSR,

and wherein, upon detection of said distributed denial of service attack, at a selected one of said specified routers all traffic received at said specified router is decoyed to said DFS, said traffic including said unicast user traffic and said unicast attack traffic.

Claim 33 (New): The system of claim 32 wherein said multicast address hopping protocol comprises: (a) varying a chosen multicast IP address selected from a plurality of multicast IP addresses according to a predetermined scheme known only to the DSF and MRS; and (b) communicating multicast packets on the chosen multicast IP address.

Claim 34 (New): The system of claim 33 further comprising a configuration file and a cryptographic key integral to said DFS and MRS for initiating said varying of said chosen multicast IP address, wherein said configuration file comprises at least one cryptographic algorithm.

Claim 35 (New): The system of claim 32 wherein said multicast capable IP network comprises at least two autonomous systems communicating by way of a border router.

Claim 36 (New): The system of claim 32 wherein said DFS further comprises a transmit address generator for generating one or more multicast addresses according to a defined set of configuration parameters, and wherein said configuration parameters comprise an address hopping order.

Claim 37 (New): The system of claim 32 wherein said DFS further comprises an IP arrival rate measuring and control system for limiting said unicast user traffic passed to said MRS.

Claim 38 (New): The system of claim 32 further comprising a control channel from said MRS to said DFS wherein, upon detection of a denial of service attack: (a) said MRS directs said PSR over said control channel to cease advertising a route to said PSSH; and (b) said MRS directs said DFS over said control channel to commence advertising a route to said PSSH.